How Leading FIs Are Using OSINT

A Financial Crime Investigator's Guide to Videris

blackdot
solutions

Contents

Introduction

Financial crime is a constant burden on individuals, organisations and governments worldwide. Estimating the precise scale of financial crime is difficult, but a recent research briefing to the UK House of Commons suggested it may reach tens or hundreds of billions of pounds per year.[1]

Businesses already spend an estimated 3% of their annual turnover fighting financial, which is necessary to prevent catastrophic financial losses, fines, and reputational damage.[2]

Existing AFC investigations and intelligence measures focus predominately on using internal banking data and manually checking watchlists or other curated data sets to identify risk. Any use of open source or live internet data to get the most comprehensive and up-to-date information is highly manual, and the approach inconsistent between institutions.

However, financial crime is characterised by the rapid development of new strategies and tactics designed to exploit financial institutions. Thus, organisations must adapt and enhance their anti-financial crime (AFC) functions to reduce risk and tackle the threat from illicit actors with greater intensity.

Influential voices within the AML/AFC community agree. In 2021, the Executive Secretary of The Financial Action Task Force stated that Financial Institutions should "stop just ticking boxes" and adopt an approach that "follow(s) the money that fuels crime and terrorism". Specifically, he suggested that FIs should take a more "intelligence-led approach", leveraging those novel tools and technologies that can

bring about a more effective way of managing financial crime risk.[3]

An intelligence-led approach demands using information drawn from all relevant sources, not just curated data sets or internal data.

Open source intelligence (OSINT) has already proven to be potent in the fight against crime on a broad range of fronts, enabling researchers to draw insights and intelligence from open source data (OSD) to learn about threat actors and their networks.

OSINT is transforming the capabilities of financial crime professionals, enabling them to more effectively screen customers and transactions, conduct enhanced due diligence (EDD) and complex investigations, and file higher quality suspicious activity reports (SARS).

What's in this guide?

Blackdot Solutions works with global organisations to help them implement Open Source Intelligence effectively.

Using our knowledge and experience of OSINT, we've put together this guide to help you understand the increasingly crucial role of OSINT in the realm of anti-financial crime (AFC). Our ultimate goal is to help you harness the power of OSINT and conduct efficient and successful investigations.

Why OSINT?

At its core, OSINT is the process by which information in the public domain is collected, analysed and turned into actionable insights. Remember, OSD includes all publicly available or publicly licensable data, including the following:

- Government sources, including crime statistics, electoral records etc.
- Corporate data in jurisdictions where this information is publicly available
- Search engine data and news media
- Grey literature
- Social media data
- Dark web data hosted on .onion domains and other darknets

The quantity of data available in the public domain has increased dramatically over the past few decades. For example, the amount of internet data created and consumed globally reached 64.2 zettabytes in 2020, and as of 2022, there are approximately 400 million active websites online.[4] While it's impossible to estimate how much internet data is considered open source, it's clear that open source data is only set to expand.

The practical uses of OSD were first realised in the 1980s when intelligence agencies started taking an interest in digital communications and the digital footprint left by internet activity. After all, the internet is primarily used by the public, and most internet data is purposefully designed for public consumption. And while internet data is not entirely immutable, permanently removing data from the public sphere is notoriously tricky.

Moreover, individual browsing habits and internet usage behaviours can be very useful to investigators. Human errors such as using the same usernames on both the surface and dark web or not stripping location metadata from uploaded files have helped law enforcement close in on international criminals and their networks. For example, several high-profile EUROPOL investigations were supported by OSINT insight into trends in criminality, digital forensics, terrorism, radicalisation propaganda, drug dealing on social networks and human trafficking.[5]

While anyone with an internet connection and browser can extract information from the internet, developing meaningful insights and answering specific questions about individuals, organisations and events requires a methodical approach to collecting, filtering and analysing data. OSINT helps to uncover deeper insights from across the surface, deep and dark web.

Today, governments and private organisations apply OSINT to a broad range of investigative, intelligence and risk management activities.

Why OSINT for AML/AFC?

The major financial crime scandals of the last decade have encouraged AML/AFC policy and process to move beyond routine automation or 'box ticking.' FIs are investing in solutions that utilise all available data, including publicly available data, to better detect and report on potentially illicit activity.

As part of this evolution, OSINT is being explicitly mentioned in the AML guidance in some jurisdictions. For example:

- **The UK Financial Conduct Authority (FCA) states in its Financial Crime Guide that FIs should integrate OSINT into EDD workflows, using "open source internet checks to supplement commercially available databases."[6]**

- **The European Banking Authority (EBA), suggests the use of "open source internet searches," and "open source data sources" in relation to undertaking EDD on transactions and transaction counterparties.[7]**

Failing to meet expectations comes at considerable cost for banks and financial institutions, who paid a combined $26 billion in fines between 2008 and 2018.[8] Alongside these regulatory pressures and the potential financial impact, businesses that knowingly or unknowingly enable financial crime and money laundering often experience higher client churn and a loss of trust amongst consumers.[9]

In the context of anti-financial crime investigations, OSINT enables teams to undertake more effective reactive investigations into customers and transactions, as well implement more proactive financial crime risk management strategies.

Reactive investigations:
OSINT can be used during reactive investigations in relation to customer screening and transaction monitoring, helping to clarify the risk profile of a company or individual, as well as verify the risk associated with a particular transaction and its counterparties.

In reactive investigations, OSINT can be used in a number of ways:

- **Corporate records can be used to verify the existence of a customer or transaction counterparty, and to better understand ownership and control structures**
- **Company websites and social media (eg. LinkedIn) can provide information that customers and counterparties release about their history and experience**
- **Adverse media searches allow online content and curated media to be searched for information that might link a customer or transaction counterparty to illicit activity, and can be weighed against the information published by the customer**

Proactive, intelligence-led investigations:
Proactive investigations are becoming more prevalent as:

- **Investigative journalists and whistle-blowers leak sensitive information into the public domain**
- **Financial information/intelligence-sharing partnerships or FISPs (whether public-private and private-private) become more widespread**

Proactive investigations evolved with the realisation that solely relying on the output of customer and transaction screening was an incomplete strategy for managing financial crime risk. Instead, FIs that adopt a proactive approach are developing teams that take their "triggers" for conducting investigations from a broader variety of intelligence sources — this approach has also become known as the intelligence-led approach.

For example, a financial crime investigations unit that adopts a proactive, intelligence-led approach might:

- **Monitor data leaks websites, the dark web, publications from specialist think tanks and research institutions, and adverse news sources for information that might connect the bank or its customers to issues that pose a reputational or legal risk.**
- **Prioritise the cultivation of positive relationships with law enforcement bodies and undertake prompt and thorough investigations following requests for information.**

Ultimately, a proactive and intelligence-led approach provides FIs with enhanced visibility and knowledge of threats, helping them take preventative measures where needed.

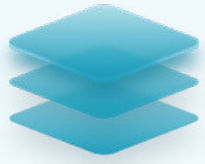
OSINT sources

Conducting successful AML investigations using OSINT requires the gathering of information and intelligence from a wide array of sources. OSD is dispersed across all three layers of the web — the surface web, deep web and dark web — extending into forums, social media and grey literature.

Understanding the basic structure of the web helps visualise the dynamics and scale of OSD:

The surface web:
The surface web is indexed by search engines such as Google and Yahoo. Search engine crawlers follow URLs and read code to understand what a web page means and index it for user retrieval in the search engine results page (SERP). The surface web is the tip of the iceberg, consisting of just 2 to 7% of the internet's total data.[10]

The deep web:
The deep web consists of 93% to 98% of all internet data. Unlike the surface web, the deep web isn't indexed by search engine web crawlers but remains open source as long as it's publicly accessible or licensable. Indexing by a search engine is immaterial in whether or not data is considered open source. Examples of deep web resources include database material, grey literature and some social media data.



The dark web:
Finally, the dark web consists of data hosted on .onion domains and other dark nets and is accessible through specialist browsers such as TOR. Roughly 1 in 20 (6.7%) of users access TOR specifically for illegal purposes, hence why dark web investigations are a major focus of cyber law enforcement teams worldwide.

Remember, the surface web isn't as straightforward as many assume due to the influence of search engine optimisation (SEO), which affects which results are shown and means that relevance is not always prioritised. The deep and dark web are less tractable, poorly structured, and cannot be searched or accessed with standard web browsers, which necessitates the use of OSINT-specific tools.

The kinds of data available across these three layers of the web include:

- **Mixed surface web data:**
  Surface web data is diverse, covering everything from blogs and forum posts to some social media data and public databases. The surface web provides an ideal starting point for many investigations.

- **Corporate records:**
  Corporate and business records can be found on both the surface and deep web and help researchers understand beneficial ownership, unusual structures, concealment of ownership, etc.

- **News and media:**
  News and media that are in front of, or behind paywalls enable researchers to build an account of a business or individual's public standing and reputation.

- **Social media:**
  Some social media data is publicly accessible and enables researchers to investigate connections between individuals and networks. For example, if a subject says that they are not connected to a PEP, but their families are friends on a social media platform, there is a clear connection that requires further investigation.

- **Addresses, phone numbers, WHOIS data and IP addresses:**
  Public data may help identify organisations, individuals and their associated physical and web properties. For example, WHOIS searches help locate registered users or assignees of internet resources.

- **Dark web data and leaks:**
  The dark web contains whistleblowing and leak platforms such as Global Leaks, NawaatLeaks, WildLeaks and WikiLeaks that can be used for OSINT purposes. Dark web marketplaces and forums also contain stolen information that can expose otherwise unknown risks.

OSINT use cases in FIs

FIs may already be using OSINT techniques within their screening and investigations activities. However, the use of OSINT within AML/AFC functions has historically been fairly rudimentary, with limited sources and unsophisticated tools being used and processes often being manual and inefficient.

In our experience dealing with FIs across the globe, use of OSINT is often confined to running customers and counterparties through PEPs and sanctions databases, as well as searching the surface web to identify information that connects the research subject to “red flag” issues. Results are then recorded in word documents and CSV files.

This approach is neither efficient nor effective, as it relies on multiple different platforms and tools to be used, and further it makes use of only a very small proportion of available data. Technology exists however that allows AML/AFC professionals to centralise a broad range of OSINT research tools all in one place, as well as make use of all relevant public data.

Let’s take a look at some of the ways FIs can utilise OSINT within their AFC investigations.

01 Simplifying due diligence

Poor or incomplete customer due diligence (CDD) and enhanced due diligence (EDD) were the most-punished AML failings between 2015 and 2020.[11] As a result, FIs now need to demonstrate the effectiveness of their CDD and EDD processes — in some cases, by extending searches into all possible sources, including OSD.

Using OSD in due diligence checks can provide additional datapoints or context, which can be used to verify bonafides or identify risk.

Let's use the example of a transaction monitoring (TM) alert identifying a corporate entity as being involved in potentially suspicious activity. The additional contextual intelligence developed from OSD can help to answer a number of questions that might allow the investigator to discount or escalate the case for further investigation:

- According to internet searches — of global news media, industry publications, NGOs and industry blogs — what is the history and general reputation of the counterparty?
- Who is/are the beneficial owner(s)?
- Is the counterparty entity connected to any other companies? What is the risk profile/ reputation of these additional entities?
- Do the transaction counterparties have a history of trading?
- Does the transaction reflect the performance, revenue and status of the counterparty?
- Does the counterparty have an easily identifiable web presence? Is it a shell company?
- Does the collected information allow the analyst to discount the alert as a false positive?

Example red flags

In each case, the investigator must make a decision based on the organisation's risk appetite, but examples of red flags that can be identified using OSINT include:

- **Unusual transactions:**
  The counterparty has engaged in an unusual transaction(s), for example, a high value/volume in comparison to its commercial history as well as review of their sales revenue and performance.
- **Complex ownership structure:**
  Counterparty has an ownership structure that is unnecessarily complex. This might include the use of offshore, inactive or shell companies.

- **PEP affiliation:**
  A potential affiliation between a customer or counterparty and a politically exposed person (PEP) or sanctioned entity is uncovered.

- **High-risk countries and/or sectors:**
  Counterparty operates in/has strong links to a high-risk country, or in a sector that is attractive to money laundering.

- **Suspected terrorist financing:**
  The customer or counterparty is suspected of links to terrorism/terrorist financing.

- **Recurring address:**
  Large numbers of companies are incorporated at the same address as the counterparty.

Identifying these red flags through OSINT-led activities can help investigators understand whether an entity warrants further investigation.

In addition, information located during an initial screen often links naturally to other relevant data, forming an auditable research trail that can be reviewed and analysed later in the investigation. Crucially, effective OSINT goes beyond the surface web to answer the above questions and uses all relevant OSD.

02 Complex investigations

Beyond fairly standardised and routine screening of customers, or the investigation of alerts generated by transaction monitoring systems, AML/AFC functions may also undertake "high risk/complex investigations".

The triggers for complex case investigations can come from a range of areas, including:

Internal SAR referrals:
Where potentially suspicious activity is identified by screening and due diligence teams, or where the investigations of transaction alerts indicates that counterparties may be operating as part of sophisticated network cases may be referred to complex case teams for review.

Media monitoring:
Allegations of criminal activity from reputable media sources can be used as intelligence, triggering proactive investigations. These activities involve the use of key sources like reports from the Organised Crime and Corruption Reporting Project (OCCRP), the International Consortium of Investigative Journalists (ICIJ), and help to develop auditable research trails that can be assessed against allegations of financial crime.

Thematic assessments:
It is becoming increasingly common for AML/AFC functions to run proactive investigations based on key typologies or thematic areas, such as "human trafficking" or "sanctions violations". These thematic reviews can be influenced by information received from a range of sources, such as:

- Publications and papers released by supranational and international bodies such as FATF and EUROPOL.
- Reports from public-private partnerships, and other law enforcement data.
- Review of sanctions watchlists.

Example of how OSINT can be applied in complex investigations

All of these activities undertaken by complex case teams can lead to the identification of previously unknown risks. However, to be done effectively, they require a combination of comprehensive data collection and management, including exploitation of external or publicly available information, as well as sophisticated analytical techniques.

This process essentially involves 4 steps:

1. Intelligence development:
OSD is collected and reviewed to gather information about allegations, typologies, groups and specific actors to better understand how organised networks of bad actors operate.

2. Network analysis:
Intelligence is developed further by analysing corporate structures and networks of individuals and entities. Visualisations are built to simplify analysis and highlight potential points for further investigation.

3. Touchpoint analysis:
The names of individuals or companies are cross-referenced against customer data to identify any overlap (or "touchpoints"), or to identify a customer's proximity to illicit actors and networks.

4. Feedback:
Once these complex investigations have been undertaken, intelligence should be shared and disseminated to relevant stakeholders and departments. This research involves the breaking down of silos and the integration between different operations, security, and risk management teams, mobilising intelligence assets to those who require them.

This final stage is often overlooked but is crucial to the development of truly effective AFC functions:

- Knowledge sharing is crucial to maximising insights gained and thematic assessments and disseminating findings and lessons learned.
- The development of internal knowledge-sharing websites and/or newsletters is key.
- FIs should create up-to-date information on country-specific red flags, indicators per financial crime typology, training material and lessons learned.
- Knowledge guides future strategy — FIs should use their proactive insights to analyse the risk of future business operations.
- Indicators can be developed from open and closed thematic intelligence to detect further unusual and suspicious activity.

03 Using external OSINT to form and prompt investigations

In addition to conducting OSINT investigations around known entities, OSINT can form and prompt intelligence-led investigations for proactive risk management. An example of this is thematic risk assessment, which enables FIs to analyse and understand financial crime typologies in the context of their business operations.

A thematic assessment of money laundering risks associated with a specific jurisdiction can inform future business operations with customers or businesses from that jurisdiction. For example, the Pandora Papers identified South Dakota as a $367 billion tax haven. Leaks and exposés should prompt FIs to analyse business associations with risky jurisdictions proactively.

OSINT enables the transition towards an intelligence-led approach to financial crime risk management:

- **Industry voices are pushing an intelligence-led approach to help FIs detect and understand financial crime threats before they develop.**
- **Proactive financial crime detection should be based on thematic risk identification rather than reactive risk identification (such as transaction monitoring).**
- **An effective financial crime intelligence model should gather and analyse intelligence proactively to understand, detect and mitigate ongoing financial crime risks.**

Overcoming common OSINT challenges

Over the past couple of decades, OSD has developed into an extensive resource. To make use of all relevant sources, OSINT researchers need to start using innovative tools and techniques that derive insight at scale.

Furthermore, OSINT techniques have evolved in recent years in order to leverage the internet's public data. This has however resulted in the emergence of tactical, strategic and operational challenges. The most common challenges FIs face when using OSINT in their investigations include:

1. **Volume of data:**
   The internet's massive scale is a double-edged sword. OSINT is effective because of the scale of the internet, but sifting through a huge range of disparate data sources is difficult and defies manual handling.

2. **Accuracy:**
   Sorting out genuine, reputable information from poor or incomplete information or 'fake news' is challenging. It can be hard to guarantee the trustworthiness of an internet domain. Identifying links between disparate information is also challenging for those relying on manual processes, leading to a risk of failing to identify important details.

3. **Consistency:**
   FIs need to be able to demonstrate a clear and effective AFC process to regulators, but the disparate and dynamic nature of open source data makes this difficult.

4. **Transparency:**
   Investigators need to be able to capture and provide evidence quickly and reliably while building a compliant audit trail. Data found online can change rapidly — for example, when a tweet is taken down or a webpage or forum post is deleted — and this needs to be managed throughout the OSINT process. Moreover, regulators such as FINCEN in the US demand organisations provide accurate references with their SARs.

These challenges are not insurmountable when investigators have access to the correct tools. Modern OSINT tools such as Blackdot Solutions Videris intelligence platform enable FIs to harness the potential of OSD while mitigating operational challenges.

Case study | Danske Bank

In order to strengthen financial crime detection, prevention and investigation capabilities, Danske Bank wanted to improve OSINT investigation capabilities to support suspicious activity report investigations.

The Challenge

Previously, OSINT was performed by investigators utilising manual Google searches to collect relevant information. This process limited investigators' access to data and produced inconsistent results, which in turn affected the ability to identify all potential risks a customer posed to the Bank.

The Solution

Danske Bank partnered with Blackdot Solutions to implement Videris to enhance the existing OSINT capabilities available to the Bank. Videris offers a holistic OSINT solution for investigations — bringing together multiple open source datasets including:

- **Search engine results**
- **Global corporate records**
- **Sanctions and PEP watchlist data**

Additionally, Videris enables investigators to search for and collate OSINT data in a single location and analyse it using inbuilt analysis and visualisation tools. Videris also provides a secure, collaborative, auditable and anonymous environment to perform open source research, enriching the Bank's OSINT investigation process to ensure risks can be more easily identified.

> Videris has supported strengthening of our Financial Crime investigation function by providing us with more enhanced OSINT capabilities that enable our investigators to identify risks faster
>
> **Marjo Pikkukangas** | Group Head of Suspicious Activity Reporting

The Benefit

The benefits delivered to Danske Bank through the use of Videris include:

- **Improved identification of risks:**
  By providing investigators with access to a wide range of open source data sets and enhanced analysis capabilities, they are able to identify previously unknown risks and assess the impact these risks may have quicker.

- **Single platform:**
  Investigators can perform an entire OSINT investigation in a single tool and collaborate with other investigators on the same case across teams – thereby streamlining both the time taken to complete an investigation and improving the depth of investigations.

- **Increased efficiency and effectiveness:**
  Videris automates time-consuming manual processes, whilst still allowing the investigator to identify key points of interest and make investigation strategy decisions (i.e.: what information to research further, when, etc.) more efficiently and effectively.

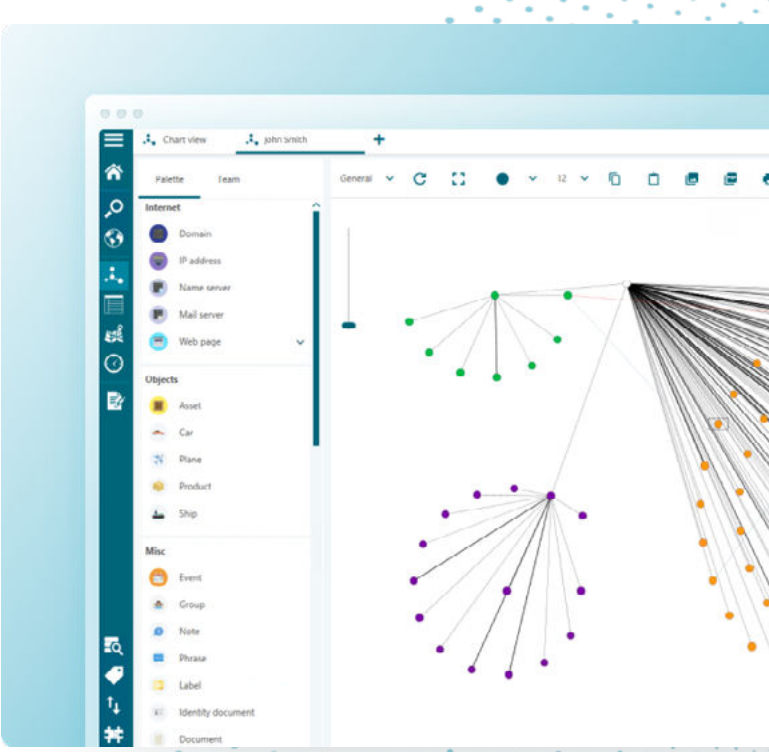
Master the use of OSINT for AFC with Videris

Videris is a holistic intelligence platform designed for the integration of both open source data and internal data. It combines all the functionality crucial to a successful OSINT investigation into a single, secure, cutting-edge ecosystem.

Videris supports complex investigations

Videris supports investigators to create a seamless workflow for efficient intuitive collection, visualisation and analysis of OSINT data.

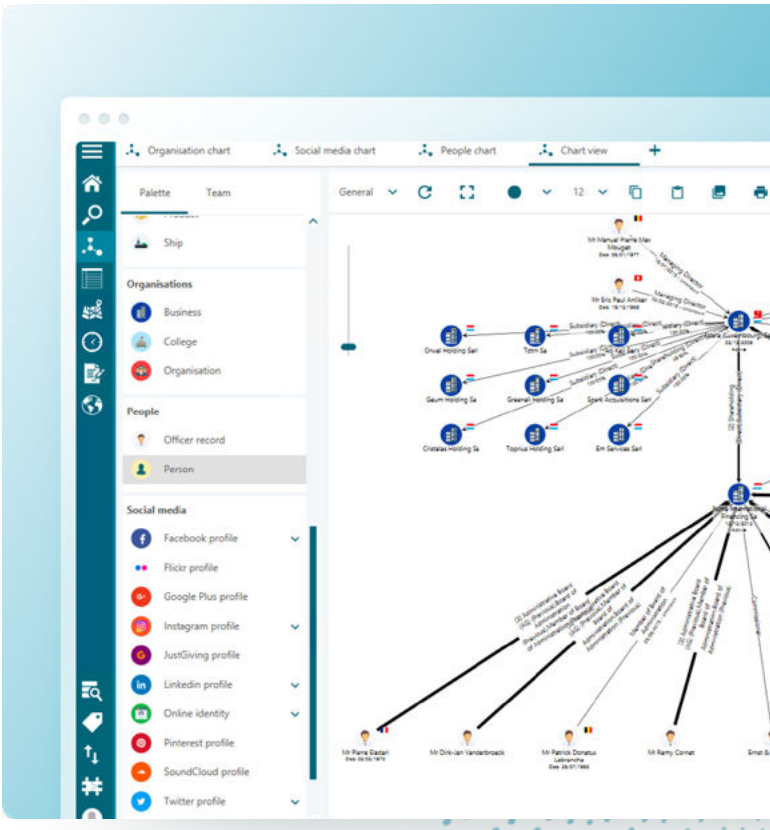
Blackdot designed Videris with human teams in mind. While the platform incorporates intelligent automation (IA) features such as entity extraction and cross-matching, we wanted to maintain the skill and sovereignty of human decision-making. As a result, Videris automates time-consuming tasks but doesn't make decisions on behalf of investigators.



Holistic analysis

Videris's ability to extend searches into multiple disparate sources within a single interface creates meaningful, overarching analysis of a subject or entity. Once researchers build a comprehensive profile for their investigation using Videris Search, they can drill down into more granular connections using visualisations and analytical tools.

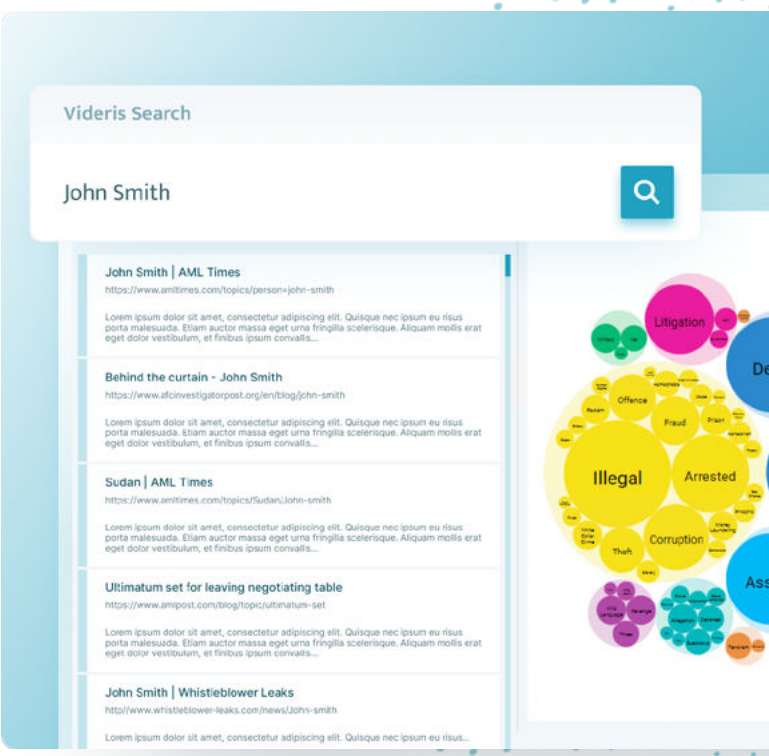
In the context of financial crime, Videris enables researchers to map networks, conduct touchpoint analysis, investigate links between businesses, individuals and entities, and discover useful corporate records and grey literature. Videris also enables the proactive investigations that regulators now expect, providing organisations with an opportunity to analyse relevant crime typologies and risks thematically.



Automated sourcing and logging

Conducting in-depth OSINT investigations in financial institutions requires the robust recording of every step undertaken and the analysis of all results that emerge. Authorities and regulators require FIs to provide specific information in SARs and other reports, including full referencing — locating information and failing to log its source renders the information useless.

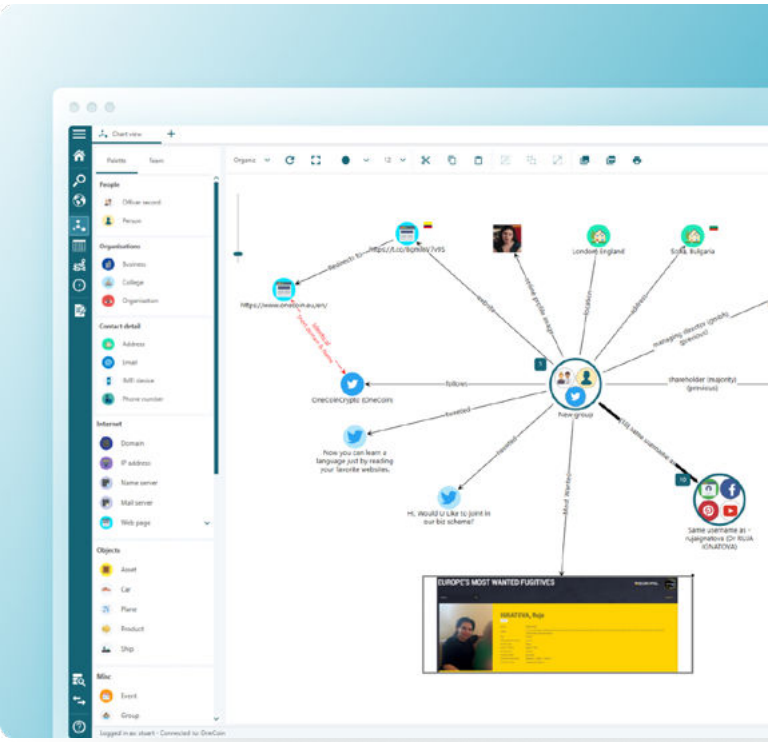
Fortunately, Videris solves these issues. Users can simply record the source of any information that is collected whilst all of the investigator's actions are simultaneously logged for future reference.



Visualisation tools

Complex networks are difficult to understand without effective visualisation. With Videris Charts, it's much easier to map information gathering during an investigation and highlight hidden connections that might otherwise be missed. These findings can then also be exported to help support internal and external reviews.

Videris also ensures investigators no longer have to analyse high volumes of information manually. Instead, you can find crucial content at speed using pre-loaded risk searches and highlighted risk terms.



Get started with Videris

Videris is already helping FIs utilise the vast volumes of publicly available data to conduct more efficient research and investigations. Book a demo today and see how Videris can augment your FIs teams investigations and produce better outcomes.

Book a demo

References

[1] Commons Library - Economic crime in the UK

[2] Refinitiv - Counting the true cost of economic crime

[3] FATF calls for the end of AML 'box ticking'

[4] Web Tribunal - How many websites are there?

[5] EUROPOL OSINT Conference

[6] FCA Handbook

[7] Final Report on Guidelines on revised ML TF Risk Factors

[8] Fenergo - Global Financial Institutions Fined $26 Billion for AML, Sanctions & KYC Non-Compliance

[9] Revealing the true cost of financial crime

[10] CS Online - What is the dark web?

[11] Financial Times - Fines for money laundering